CONTINUATION OF APPLICATION FOR SEARCH WARRANT

I, Tom Peller, being first duly sworn, hereby depose and state as follows:

1. I make this continuation of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the cell phone ending in 4601, "**Target Phone",** seized from the person of Lorenzo Lamarr Naylor at the time of his arrest, as further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since 2018. I am currently assigned to the FBI's Detroit Cyber Division. My current duties involve investigating crimes involving computer fraud, wire fraud, money laundering, identity theft, child exploitation, internet stalking, and conspiracies to commit those crimes. I have a Bachelor of Science Degree in Mathematics, a Master's Degree in Statistics and Actuarial Science, and approximately three years of professional experience as an Actuarial Analyst and Data Scientist in private industry. Additionally, I have received specialized training in the FBI relevant to the investigation of computer related crimes.

3. The facts in this Continuation come from my personal observations, my training and experience, and information obtained from other agents, investigators, and witnesses. This Continuation is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this Continuation, there is probable cause to believe that violations wire fraud (18 U.S.C. § 1343), money laundering (18 U.S.C. § 1956), and conspiracy (18 U.S.C. § 371) have been committed by Lorenzo Naylor (hereafter "Naylor"). There is also probable cause to search the **Target Phone**, further described in Attachment A, for evidence, instrumentalities, and/or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

6. In March 2022, the Marquette, Michigan sheriff's office referred a case to the FBI related to the sex-based extortion and suicide of a victim in the Western District of Michigan, J.D., who was a 17-year-old high school student. The investigation revealed that on March 24/25, 2022, an Instagram user with username "dani.robertts" solicited child pornography from J.D. and then threatened to release it unless J.D. paid money. J.D. initially paid $300, but dani.robertts demanded more. J.D. threatened to commit suicide, and dani.robertts encouraged him to do so. J.D. then committed suicide.

7. The investigation into this incident led to the identification of a broader Nigeria-based "sextortion" ring composed of a hacking, money laundering, and online sex-based extortion. In January and February 2023, the Nigerian Economic and Financial Crimes Commission arrested six men in Nigeria in coordination with the FBI. Four of these men are named Samuel Ogoshi (hereafter "Samuel"), Samson Ogoshi (hereafter "Samson"), Francis Ekpe (hereafter "Ekpe"), and Ezekiel Robert (hereafter "Ezekiel").

8. Ekpe was the money launderer of the ring. In February 2023, another FBI Agent and I interviewed Ekpe in Lagos, Nigeria. Ekpe described to me that his job in the sextortion ring was to provide financial accounts of U.S.-based individuals to the sextortionists, so they had the ability to move their victim's money from the U.S. to Nigeria. Ekpe described his process during the interview, which was the following: Ekpe initially recruited people from the U.S. on Telegram. Then the U.S. people would bring in other friends and put them in touch with Ekpe.

- The U.S. people provided their electronic payment accounts (i.e. Apple Pay, CashApp, Zelle, PayPal, etc.) to Ekpe.

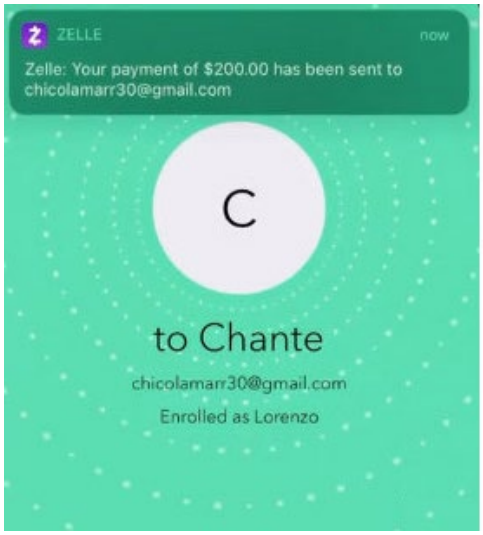
- Ekpe provided those accounts to the sextortionists, who if the extortions were successful, would get the victims to deposit money into them.
- Ekpe notified the U.S. persons when this occurred and told them to keep 20% of the money as their cut.
- The U.S. persons converted the remaining 80% to Bitcoin and sent it to him.
- Ekpe received the Bitcoin through his Binance1 account and then would use Binance's P2P (Peer to Peer) platform to convert the victim money to Nigerian Naira.
- Ekpe would then send the Nigerian Naira to the sextortionists and keep a fee for himself based on the conversion rate.

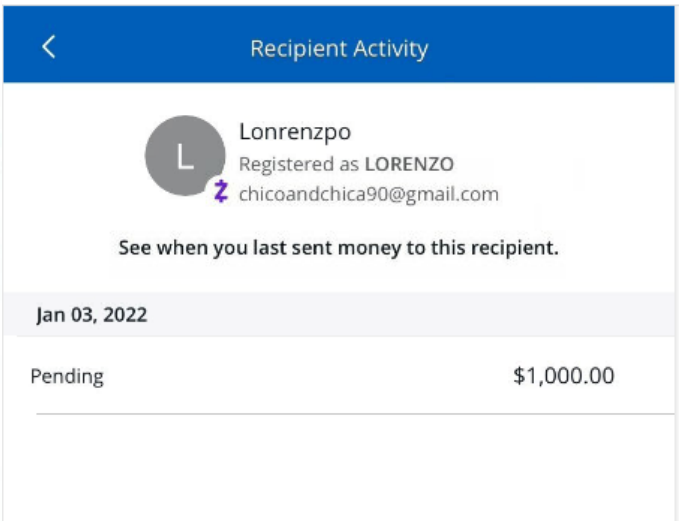
9. Ekpe identified U.S. persons he worked with in his money-laundering scheme, three of whom were Johnathan Green (hereafter "Green"), Kendall London, (hereafter London") and Brian Coldmon (hereafter "Coldmon"). I also saw that Naylor was listed as a contact in Ekpe's phone with the same phone number as the **TARGET PHONE**.

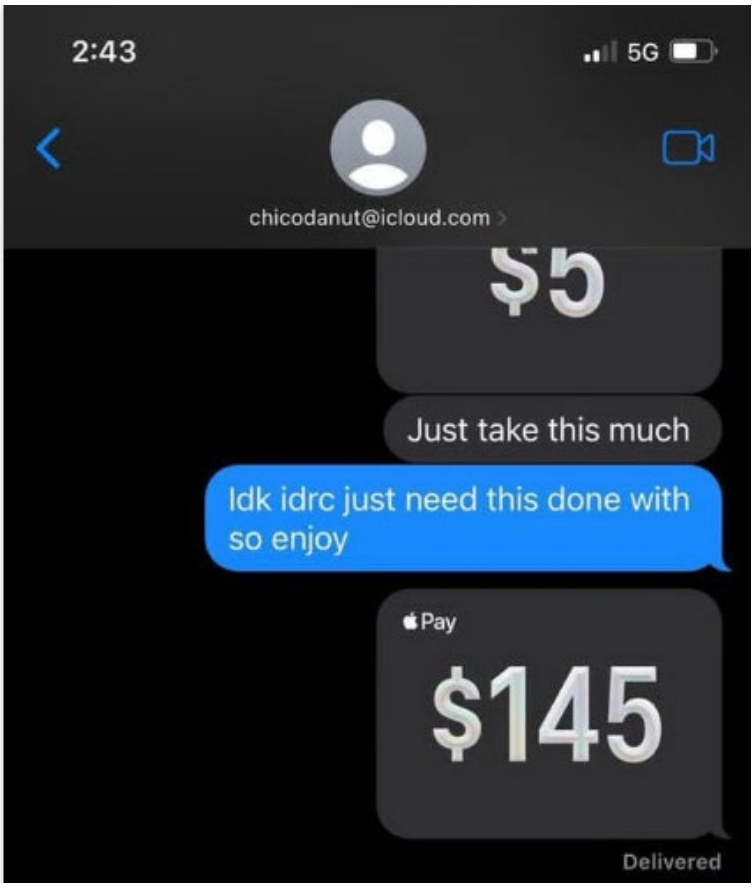
10. As mentioned in paragraph 6, J.D., prior to his suicide, made a $300 extortion payment via Apple Pay. I saw that this payment was made to the Apple Pay account of Green. Further, I learned that on the same night, Green received an additional $300 in extortion payments from another identified victim of sextortion into his same Apple Pay account. Green then transferred the $600 to his CashApp account, less a transaction fee. From there, Green transferred approximately 20% of the victim money to another CashApp account under his control and converted the remaining funds to Bitcoin. Finally, he sent the Bitcoin to Ekpe's identified Bitcoin address at Binance.

11. I requested and received records from Binance regarding Ekpe's Bitcoin activity. From the records, I identified two primary accounts associated with Ekpe ("Crypto Account 1") and (Crypto Account 2"). I analyzed the deposit activity in Crypto Account 1 and Crypto Account 2 and saw that between March 2021 and May 2022, Ekpe received more than 580 deposits that totaled the equivalent of approximately $250,000 in Bitcoin. I recognized the average amount of deposit, approximately $431, as being an amount similar to that of a sextortion payment.

12. Prior to the arrests of the six men in Nigeria, the case team served search warrants on the Google emails and Apple iClouds associated with Samuel, Samson, Ekpe, and Ezekiel. I reviewed each of these emails and iClouds and found numerous screenshots of financial activity, which I now know to be victim extortion payments. While reviewing the screenshots, the case team identified a series of email addresses of the U.S.-based people who moved money for Ekpe. Specifically, I found screenshots of payments made to chicolamarr30@gmail.com, chicoandchica90@gmail.com, and chicodanut@icloud.com, email addresses associated with Naylor. Examples of these can be seen below:







13. I subpoenaed CashApp for transactional information associated with Naylor. From the return, CashApp associated Naylor with the phone number of the **Target Phone**. The "cashtag" name associated with Naylor's CashApp account was "chicodanut" and the display name was "Chico Taylor". I recognized "chicodanut" as being the same prefix to the email address shown above, chicodanut@icloud.com. Additionally, I found approximately 30-40 Bitcoin transactions sent from Naylor to Ekpe, indicating he laundered dozens of likely sextortion or other fraud victim payments on behalf of Ekpe. Since Ekpe was located in Nigeria during the time of these transactions, I know from my training and experience, as well as from my knowledge of the case, that Ekpe utilized internet-based chat applications and features such as iMessage, WhatsApp, and TextNow to communicate with the U.S.-based money launderers. Thus, since Naylor sent dozens of Bitcoin transactions to Ekpe and since the phone number of

the **Target Phone** was listed as a contact in Ekpe's contact list, there is probable cause that Naylor utilized the **Target Phone** to communicate with Ekpe and facilitate the movement of fraud money from the United States to Nigeria.

14. In July 2024, I served search warrants to Apple and Google for the accounts related to Naylor, as mentioned in paragraph 12. I reviewed the returns from Apple and saw communications between victims of sextortion and Naylor. Specifically, I saw communications where they discuss the amount of money to send to Naylor because of the extortion.

15. As part of this investigation, I interviewed two conspirators who knew Naylor. The two conspirators said that Naylor went by the nickname "Chico". They each advised that they were part of introducing Naylor to "the plug", who I know to be Ekpe. Specifically, one told me that Naylor moved money for Ekpe and Naylor knew the money was associated with fraud. The conspirators also confirmed the phone number for Naylor was that of the **Target Phone**.

16. In April 2025, FBI agents from the Atlanta field office interviewed Naylor's assigned probation officer. Naylor's probation officer confirmed Naylor's phone number was that of the **Target Phone.**

17. On May 15, 2025, I, along with other FBI agents, arrested Naylor in the Atlanta, Georgia, area after he was indicted in the Western District of Michigan on the charge Conspiracy to Commit Wire Fraud (Case No. 2:25-CR-6). At the time of his arrest, Naylor was in possession of the **Target Phone**. I accompanied Naylor while he was transported from the site of his arrest to the federal courthouse in Atlanta. During the transport, I advised Naylor of his rights. Naylor said he understood his rights, signed a consent form, and stated that he wanted to speak with me. During the interview, Naylor gave me the passcode to the **Target Phone** and allowed me to

unlock it. Naylor directed me to the CashApp application on his phone. He had me sign out of one of his accounts and log into another. I saw that the other account was in the name "Chico Taylor" and the cashtag associated with it was "chicodanut". I recognized both "Chico Taylor" and "chicodanut" as being the same identifiers from the CashApp subpoena return where I identified Bitcoin transfers to Ekpe.

18. While Naylor gave me permission to access his CashApp application, he declined to give me written consent to seize and search the **Target phone**. I advised Naylor that I was going to secure the Target phone in anticipation of obtaining a search warrant. The **Target phone** was secured in Atlanta Field Office and then transferred to the Grand Rapids Resident Agency where I will be able to coordinate a forensic examination. I turned the Bluetooth feature off and placed the **Target phone** in airplane mode to prevent changes on the device.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

19. As described above and in Attachment B, this application seeks permission to search the **Target Phone**. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

20. *Probable cause.* I submit that evidence of the crimes under investigation will be stored on the **Target Phone**, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a modern cell phone can be stored for years at little or no cost. Even when files have been deleted,

they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a cell phone, the data contained in the file does not actually disappear; rather, that data remains on the cell phone until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the cell phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a cell phone's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, cell phone storage media—in particular, cell phones' internal hard drives—contain electronic evidence of how a cell phone has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Cell phone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic data that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how any cell phones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the **Target Phone** because:

a. Data on the cell phone can provide evidence of a file that was once on the cell phone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the cell phone that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the cell phone that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the cell phone was in use. Electronic file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a cell phone and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a cell phone or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the cell phone or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the cell phone was remotely accessed, thus inculpating or exculpating the cell phone owner. Further, cell phone activity can indicate how and when the cell phone or storage media was accessed or used. For example, as described herein, cell phones typically

contain information that log cell phone user account session times and durations, cell phone activity associated with user accounts, electronic storage media that connected with the cell phone, and the IP addresses through which the cell phone accessed networks and the internet. Such information allows investigators to understand the chronological context of cell phone or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a cell phone or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a cell phone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the cell phone user. Last, information stored within a cell phone may provide relevant insight into the cell phone user's state of mind as it relates to the offense under investigation. For example, information within the cell phone may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a cell phone works can, after examining this forensic evidence in its proper context, draw conclusions about how cell phones were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a cell phone that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, cell phone evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a cell phone is evidence may depend on other information stored on the cell phone and the application of knowledge about how a cell phone behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a cell phone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

22. *Necessity of seizing or copying entire cell phones or storage media.* In most cases, a thorough search of a person or premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the cell phone's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a cell

phone has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of cell phone hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

23. *Nature of examination.* Based on the foregoing and consistent with Rule41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying the **Target Phone** that reasonable appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to

computer-assisted scans of the entire cell phone, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

24. Based on the above information, I respectfully submit that there is probable cause to believe the crimes of wire fraud (18 U.S.C. § 1343), money laundering (18 U.S.C. § 1956), and conspiracy (18 U.S.C. § 371) have been committed by Naylor and that evidence, instrumentalities, and fruits relating to this criminal conduct, as further described in Attachment B, will be found on the **Target Phone**.